Innføring av PSD2 i Norge:

PSD2 endrer finansbransjen

Payment Services Directive 2 (PSD2) er starten på en ny fremtid for finansbransjen. Tiden der vi gjør alle våre finansielle transaksjoner via banken, er forbi. PSD2 åpner opp for helt nye muligheter, og for noen vil det nye regelverket bety helt nye mulige forretningsområder.

Leder for Digital Trust
Lars Erik Fjørtoft
Partner PwC

Advokat
Daniel Næsse
PwC

Dette skjer fordi endringer i regelverket for betalingstjenester gir adgang for tredjeparter til å tilby tjenester basert på tilgang til kundens konto hos en tradisjonell bank.

Fristen for gjennomføring av direktivet i EU var 13. januar 2018, men i Norge ble implementering utsatt til 1. april 2019. Dette innebærer forandringer i finansforetaksloven og tilhørende forskrifter, som åpner for nye typer konsesjoner og betalingstjenester.

Nye betalingstjenester og typer av konsesjoner

Betalingsfullmaktstjenester og kontoinformasjonstjenester
Fra 1. april innføres to typer fullmaktstjenester – betalingsfullmaktstjenester og kontoinformasjonstjenester. Betalingsfullmakttjenester innebærer at kunden gir en tredjepart fullmakt til å få utført betalinger fra kundens konto i en bank («kontotilbyder»), mens kontoinformasjonstjenester er tjenester hvor kunden gir en tredjepart fullmakt til å innhente opplysninger om kundens konto hos en eller flere kontotilbydere og sammenfatte/konsolidere disse opplysningene.

Fullmaktsforetak
Tilbydere av disse tjenestene omtales som «fullmaktsforetak» i kommende regelverk. Tjenestene vil defineres som «betalingstjenester» etter finansavtaleloven.

Betalingsfullmektig og opplysningsfullmektig
Fra 1. april vil det også være mulig å oppnå konsesjon som «betalingsfullmektig» og «opplysningsfullmektig» i Norge.

Foretak med konsesjon som «betalingsfullmektig» (Payment Initiation Service Provider – PISP) reguleres som «betalingsforetak» etter finansforetaksloven § 2–10.

Betalingsforetak som kun har konsesjon for betalingsfullmaktstjenester, unntas fra lovens regler om kapitalkrav og sikring av kundemidler, men omfattes av egne krav til ansvarsforsikring. Forsikringsdekningens omfang skal beregnes etter EBAs Guideline (2017/08) om dette. I tillegg etableres et eget startkapitalkrav for betalingsfullmektig på EUR 50 000.

Et foretak som har fått fullmakt fra kunden til å innhente opplysninger om sine konti hos en eller flere andre kontotilbydere, omtales som en «opplysningsfullmektig» (Account Information Service Provider – AISP). Tjenesten(e) som utføres av foretaket omfattes av ny konsesjon i § 2–10 a i finansforetaksloven.

Foretak som kun skal yte disse tjenestene, unntas fra ytterligere krav etter finansforetaksloven, herunder om eierforhold, kapitalkrav og tiltak for å oppfylle krav etter hvitvaskingsloven.

For opplysningsfullmektigene gjelder ikke noe eget kapitalkrav, men disse skal etablere ansvarsforsikring beregnet etter EBA Guideline nevnt ovenfor. Opplysningsfullmektiger kan etableres som enkeltmannsforetak.

Forholdet mellom kontoførende bank og fullmaktsforetakene

Tilgang til kundenes konti uten avtale med kontotilbyder
Bankene må fra 1. april gi foretak med tillatelse for å tilby ovennevnte tjenester tilgang til felles kunders konti i banken. I praksis vil dette skje ved at fullmaktsforetaket kobler seg opp elektronisk via et såkalt «API» (Application Programming Interface) og ber om tilgang. I henvendelsen vil foretaket identifisere seg overfor banken som et foretak med nødvendig konsesjon. Bankene vil måtte akseptere slike henvendelser, uten at det foreligger noen avtale mellom banken og fullmaktforetaket. Dette gjelder for alle foretak med konsesjon i et EU-land, og for både privat- og bedriftskunders konti.

Konkurransen om å være kundenes foretrukne betalingsløsning/«ordrekanal» vil nå frikobles fra hvilken bank kundens konto er plassert hos.

Lik behandling av kundens ordre – uavhengig av «plattform»

En vesentlig regel er at kontoførende bank ikke kan differensiere (diskriminere) kundens ordre fordi den kommer via en tredjepart. Det skal ikke ha noen betydning for verken tilgangs-/autentiseringsløsning, pris eller hurtighet i behandling av ordren om kunden gjør den i kontoførende bank sin app/nettbank eller via en app (eller annen kanal) levert av tredjepart.

Det er bankene som velger hvilken autentiseringsløsning som skal benyttes for å kontrollere at et fullmaktsforetak har fullmakt fra kunden. Henvendelser via fullmaktsforetak skal som nevnt over likevel ikke diskrimineres/vanskeliggjøres i forhold til henvendelser i «bankens kanaler». Derfor må bankene tilby fullmaktsforetakene tilgang til de autentiseringsløsningene som banken benytter.

At bankene ikke kan gjøre betalingsordre mottatt «direkte» fra kunden på bedre betingelser, får bankens tjenester til å ligne på «infrastruktur» – tilgjengelig for alle. Det er riktignok bankens egen beslutning om den vil ta betalt for å utføre en betalingsordre, men det må være like vilkår også hvis kunden benytter et fullmaktsforetak.

Dette gjør at konkurransen om å være kundenes foretrukne betalingsløsning/«ordrekanal» vil være frikoblet fra hvilken bank kundens konto er plassert hos. På det viset blir markedet for betalingstjenester og markedet for bankkonti i prinsippet uavhengig av hverandre.

Ansvarsforhold mellom fullmaktsforetak, kontoførende bank og kunde

For kundenes del er det ikke store endringer i norsk regelverk på dette området. Kundens ansvar for tap ved stjålet eller tapt betalingsinstrument iht. finansavtaleloven § 35 (2) reduseres fra kr 1200 til kr 400.

Ansvarsfordeling mellom betalingsfullmektig og kontoførende bank overfor kunden er imidlertid et nytt område, og her inneholder nytt regelverk bestemmelser for uautoriserte transaksjoner og transaksjoner som ikke gjennomføres korrekt.

Utgangspunktet er at kontoførende bank har ansvar for umiddelbart å tilbakeføre uautoriserte betalinger eller ikke korrekt gjennomførte betalinger til kundens konto.

Som i dagens regelverk, finansavtaleloven § 35 (5), er det finansforetaket – ikke kunden – som har ansvar for å dokumentere at betalingen er korrekt autentisert og ikke rammet av teknisk svikt eller annen feil. Dersom betalingen er initiert via et fullmaktsforetak, er det imidlertid nå dette foretaket som har bevisbyrden. Betalingsfullmektigen har bevisbyrden for at transaksjonen var korrekt autentisert, registrert og ikke rammet av teknisk svikt på betalingsfullmektigens område. Kontoførende bank kan deretter eventuelt gjøre regresskrav gjeldende mot betalingsfullmektigen.

De nye bestemmelsene regulerer også foretakenes opplysningsplikt og øvrige forpliktelser overfor kundene, samt at det stilles krav til hvilken informasjon bankene skal yte betalingsmottakere og fullmaktforetak i forbindelse med en transaksjon.

Regler om sikker kommunikasjon og sterk kundeautentisering

EU-kommisjonen har fastsatt egen forordning om hvordan banker og fullmaktsforetak skal kommunisere sikkert med hverandre og med kundene. Denne trer ikke i kraft før 14. september 2019. Det foreligger ikke noe utkast til norsk oversettelse, men Finanstilsynet bekrefter at norske regler tilsvarende denne forordningen vil gjelde fra samme dato.

I ny forskrift om systemer for betalingstjenester § 5 innføres likevel et krav til «sterk kundeautentisering» for alle betalingstjenestetilbydere, når kunden:

«a) logger seg inn på sin betalingskonto via nettet,

b) initierer en elektronisk betalingstransaksjon, eller

Betydningen for regnskapsførere og revisorer

For regnskaps- og revisjonsbransjen og tilhørende systemleverandører kan det også oppstå nye muligheter som følge av PSD2. Der bransjen tidligere har måttet basere seg på bilaterale avtaler med hver enkelt bank for å kunne få innsyn i og eventuelt adgang til å legge inn belastninger på kundenes konti, vil man nå potensielt kunne oppnå slik tilgang ved hjelp av konsesjon som fullmaktsforetak og etter fullmakt fra kunden.

Dette betyr at det ikke er behov for avtale mellom regnskapsfører/revisor/systemleverandør og hver enkelt kontoførende bank. Hvorvidt det vil være begrensninger i forhold til å inneha såpass forskjellige typer av konsesjon som dette innebærer, vil eventuelt måtte vurderes av Finanstilsynet i tiden fremover.

Det er flere aktører som jobber med å utforske muligheter her, blant annet vi i PwC. Det er dog lite trolig at PSD2-konsesjon vil gi tilstrekkelige tilganger for vårt behov som revisor, til det vil PSD2-API'ene bli for smale. PSD2 gir også kun tilgang til informasjon på betalingskonti og ikke andre plasseringskonti, lån mv. De bilaterale avtalene vil nok dermed i første omgang fortsatt være relevante, iallfall frem til neste fase av «open data»-arbeidet under EUs Digital Single Market-paraply. Det er nemlig ikke usannsynlig at EU etterhvert også vil stille krav til at bankene/finansinstitusjonene må åpne for tilgang via API'er til andre typer konti og tjenester: lån, plassering, pensjon, forsikring mv. Dette vil være en neste fase som har et enda større potensial enn det vi får med dagens PSD2-innføring.

c) gjennomfører handling som kan innebære risiko for svindel eller annet misbruk.»

Ettersom forskriften trådte i kraft 1. april, vil dermed kravet til «sterk kundeautentisering» gjelde i Norge allerede fra denne datoen.

Med «sterk kundeautentisering» menes «en løsning basert på bruk av to eller flere elementer, som er uavhengige av hverandre slik at kompromitteringen av ett element likevel ikke vil påvirke de andre elementene».

Ved betalinger skal slik autentisering også «koble transaksjonen til et spesifikt beløp og en spesifikk betalingsmottaker» – dvs. inneholde samtykke til den konkrete transaksjonen.

Beskyttelse av kundenes sikkerhetsinformasjon og «screen scraping»

Ny forskrift om systemer for betalingstjenester § 11 pålegger på den annen side betalingstjenestetilbydere å sikre at brukerens personlige sikkerhetsinformasjon ikke blir tilgjengelig for andre enn brukeren, når den aktuelle identifikasjonen eller signaturen også gir adgang til elektroniske tjenester fra offentlig sektor. Dette medfører antagelig at «screen scraping»[1] ikke vil være aktuelt i Norge i perioden frem til 14. september 2019, på tross av at EBA tidligere har uttalt at dette må tillates av bankene i denne perioden.

Overgangsordninger

Endringene medfører at også etablerte betalingsforetak vil omfattes av en rekke nye krav til virksomheten.

Finansforetaksforskriften inneholder overgangsordninger for de etablerte foretakene, som må innordne seg nye krav innen ulike frister.

Hva betyr dette for kundene og for bankene?

For kundenes del betyr endringene at det blir mindre viktig hvilken bank man velger å ha konto i, i hvert fall i forhold til betalingstjenester. Om du har konto i bank A, B eller C kan du likevel benytte kun Bank C til alle betalinger og få en samlet oversikt over saldo fra alle konti. Alternativt kan du benytte en tjenesteleverandør som kanskje ikke er en bank, men som kun tilbyr fullmaktstjenester.

1 Fra Wikipedia: Skjermskraping, av engelsk screen scraping, vil si å kopiere tekst og medieelementer fra eksterne kilder for å ekstrahere nyttig informasjon. Vanligste form er skraping av nettsider.
Skjermskraping benyttes ofte for å koble ulik informasjon fra ulike nettsteder og skal bøte på at nettstedene som kobles, ikke har lagt ut informasjonen i strukturerte tekstformater som gjør kobling enkelt.

Hvordan tjenestetilbudet til kundene vil utvikle seg, er vanskelig å spå om, men i kombinasjon med «FinTech»-utvikling vil kanskje banktilbudet se helt annerledes ut om noen år. I denne sammenhengen er PSD2 bare en del av bakgrunnen som sørger for en viktig endring i rammevilkårene fordi den åpner opp for konkurranse om tilgang til kundenes konti.

PSD2 sin betydning for brukerstedene (butikkene)

Næringsdrivende i rollen som betalingsmottakere kan fortsatt inngå avtaler med alle typer betalingstjenesteaktører. En butikk kan for eksempel tilby rabatt ved bruk av Bank B sin betalingsapp eller kort. Butikkene kan dog ikke ta høyere betaling for bruk av bestemte betalingsinstrumenter/kanaler, enn hva som tilsvarer butikkens direkte økte kostnader ved bruk av dette «betalingsinstrumentet».

Konkurransen vil derfor (som tidligere) foregå mellom betalingssystemer overfor butikkene, og indirekte mellom betalingssystemer i forhold til at flest mulig kunder ønsker å benytte dem – fordi mange butikker gjør det.

Til nå har håndtering av betalingsområdet vært relativt enkelt for norske brukersteder, spesielt i dagligvare hvor betaling skjer «fysisk» i butikken. Dette

Den norske betalingsløsningen BankAxept (som nå er fusjonert i VIPPS) har vært mye billigere enn alle alternativer. Ved innføringen av PSD2 kan dette endres.

skyldes at den norske betalingsløsningen BankAxept (som nå er fusjonert i VIPPS) har vært mye billigere enn alle alternativer (i praksis VISA og MasterCard). Ved innføringen av PSD2 kan dette endres eksempelvis ved at:

- norske dagligvareaktører lager sitt eget betalingsforetak basert på PSD2 for å gjøre betalinger billigere eller med flere fordeler enn med BankAxept
- nye aktører etablerer seg basert på PSD2 og tilbyr enda bedre avtaler enn BankAxept kan tilby
- VISA/MC bestemmer seg for å re-prise sine transaksjoner/brukerstedsavtaler for å møte ny konkurranse og prioriterer å gi de risikofrie transaksjonene fra dagligvare spesielt attraktiv prising for å vinne en dominerende posisjon (utkonkurrere BankAxept)

Dagligvareaktørene jobber i disse dager med å finne gode strategier for hva de skal gjøre, blant annet koordinert gjennom deres felleseide selskap Aera (Coop og NorgesGruppen). Vi er helt sikre på at det også tenkes på hvordan man skal håndtere den nye situasjonen i VISA og MC pluss VIPPS.

En kompliserende faktor for dagligvareaktørene er at de også må ta hensyn til sitt ønske om å kunne ha en sikker ID på kunden slik at de kan fortsette å tilby gode lojalitetsløsninger (Æ, Trumf, Coop). Videre vil betalingsløsningen måtte understøtte et ønske om å gjøre dette så enkelt og friksjonsløst som mulig for kunden å bruke, ikke skape kassekø, kunne følge kundene over på netthandel mv. Betaling har med andre ord blitt en del mer komplekst for dagligvareaktørene og med mye større muligheter til å skape smarte løsninger.

PSD 2 vs. GDPR

Forholdet mellom ny personopplysningslov som gjennomfører GDPR (General Data Protection Regulation) i Norge og PSD2 har vært gjenstand for ulike diskusjoner. Problemstillingen er aktuell fordi betalingstjenesteytere (herunder fullmaktsforetak) normalt må behandle og lagre personopplysninger om både betaler og mottaker, og benytte disse til en rekke behandlingsformål, herunder eksempelvis lovbestemt plikt etter bokførings- og regnskapslovgivning. Videre er det naturlig å tro at fullmaktsforetakene vil være svært interessert i å gjøre bruk av kundeopplysninger til å tilby tjenester som forbruksanalyse, utvalgte tilbud og kampanjer, effektivisering av betalingsmønstre for den enkelte og så videre. Kun fantasien setter grenser for hva den enkeltes finansielle opplysninger kan brukes til.

Enkelte av bestemmelsene i PSD 2, eksempelvis artikkel 94 (2), skaper uklarheter med hensyn til hva som vil utgjøre grunnlag for behandling av personopplysninger for betalingstjenesteytere. I denne sammenheng har det betydning hvorvidt det såkalte «Lex Specialis»-prinsippet som innebærer at spesiell lovgivning går foran generell lovgivning på det enkelte område, kan ansees å løse spørsmål om eventuell motstrid mellom regelverkene. Dette vil ventelig bli klargjort i tiden fremover, gjennom praksis og rundskriv fra så vel norske som europeiske tilsynsorgan.

Oppsummerende betraktninger

I 2019 vil betalingsområdet endres vesentlig. Det vil komme flere aktører inn i markedet og nye muligheter vil åpnes. For oss som kunder vil det gjøre at vi får flere valgmuligheter, men det kan også øke kompleksiteten. For bankene gir det en totalt ny hverdag hvor de må åpne opp tilgangen til kundene sine for nye aktører. For brukersteder vil det også gi nye muligheter og økt kompleksitet. Innføringen kan også gi nye muligheter for regnskapsførere og revisorer for å effektivisere driften sin.

Innføringen av PSD2 medfører også at den «selvregulering» bankene har hatt historisk i Norge der de kunne bestemme over betalingsområdet mer eller mindre på egenhånd gjennom felleseide selskaper og løsninger (eksempelvis BankAxept), nå definitivt er over.